AMENDMENTS

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising a plurality of activities, comprising:
automatically:
receiving a plurality of elements for each of a plurality of continuous data streams;
treating the plurality of elements as a first data stream matrix that defines a first dimensionality;
reducing the first dimensionality of the first data stream matrix to obtain a second data stream matrix, the second data stream matrix comprising a plurality of sampled values of the first data stream matrix;
randomly computing a singular value decomposition of the second data stream matrix, a probability of computation determinable based upon a ratio of a magnitude of a sum of sampled values obtained since a prior computation of the singular value decomposition to a calculated product of a determined separating value of eigenvalues and a determined eigenvalue of the second data stream matrix; and
based on the singular value decomposition of the second data stream matrix, quantifying approximate linear correlations between the plurality of elements, the approximate linear correlations between the plurality of elements usable to automatically identify and automatically report a denial of service attack without address spoofing.

2. (Currently Amended) The method of claim 1, further comprising:
obtaining the plurality of elements, the plurality of elements stored as a collection of hash functions.

3. (Original) The method of claim 1, wherein at least one of the plurality of continuous data streams is synchronous.

4. (Original) The method of claim 1, wherein at least one of the plurality of continuous data streams is asynchronous.

5. (Original) The method of claim 1, wherein at least one of the plurality of continuous data streams is bursty.

6. (Original) The method of claim 1, wherein at least one of the plurality of continuous data streams is sparse.

7. (Original) The method of claim 1, wherein at least one of the plurality of continuous data streams comprises out of order elements.

8. (Currently Amended) The method of claim 1, wherein said reducing activity ~~applies the Johnson-Lindenstrauss Lemma~~ obtains values for the second data stream matrix from a Gaussian distribution and preserves relative distances between vectors in a resulting space of the second data stream matrix as compared to the first data stream matrix, the second matrix determined via a sliding window stream model.

9. (Currently Amended) The method of claim 1, further comprising:
repeating said computing activity, said computing activity repeated responsive to a change in the second data stream matrix caused by additional data sampled from a data stream of the plurality of continuous data streams.

10. (Currently Amended) The method of claim 1, further comprising:
responsive to an expiration of some entries in the second data stream matrix, periodically repeating said computing activity.

11. (Original) The method of claim 1, further comprising:
randomly repeating said computing activity.

12. (Currently Amended) The method of claim 1, wherein said quantifying activity occurs ~~dynamically~~ responsive to sliding window stream that varies over time.

13. (Original) The method of claim 1, wherein the approximate linear correlations comprise a plurality of eigenvalues that approximate principal eigenvalues of the first data stream matrix.

14. (Original) The method of claim 1, wherein the approximate linear correlations comprise a plurality of eigenvectors that approximate principal eigenvectors of the first data stream matrix.

15. (Original) The method of claim 1, further comprising:
receiving a user-specified accuracy metric for the approximate linear correlations.

16. (Original) The method of claim 1, wherein the approximate linear correlations meet a user-specified accuracy metric.

17. (Currently Amended) The method of claim 1, further comprising:
~~outputing~~ outputting the approximate linear correlations.

18. (Original) The method of claim 1, further comprising:
reporting the approximate linear correlations.

19. (Currently Amended) A machine-readable medium comprising instructions for activities comprising:
receiving a plurality of elements for each of a plurality of continuous data streams;
representing the plurality of elements as a first data stream matrix that defines a first dimensionality;
automatically reducing the first dimensionality of the first data stream matrix to obtain a second data stream matrix, the second data stream matrix comprising a plurality of sampled values of the first data stream matrix;
randomly computing a singular value decomposition of the second data stream matrix, a

probability of computation determinable based upon a ratio of a magnitude of a sampled value of the plurality of sampled values to a calculated product of a determined separating value of eigenvalues and a determined eigenvalue of the second data stream matrix; and

based on the singular value decomposition of the second data stream matrix, quantifying approximate linear correlations between the plurality of elements, the approximate linear correlations between the plurality of elements usable to automatically identify and automatically report a denial of service attack without address spoofing.

20. (Currently Amended) A system comprising:

a stream element processor adapted to receive a plurality of elements for each of a plurality of continuous data streams;

a first matrix processor adapted to represent the plurality of elements as a first data stream matrix that defines a first dimensionality;

a second matrix processor adapted to:

reduce the first dimensionality of the first data stream matrix to obtain a second data stream matrix;

randomly compute a singular value decomposition of the second data stream matrix, a probability of computation determinable based upon a ratio of a magnitude of a sampled value of the plurality of sampled values to a calculated product of a determined separating value of eigenvalues and a determined eigenvalue of the second data stream matrix; and

based on the singular value decomposition of the second data stream matrix, quantify approximate linear correlations between the plurality of elements, the approximate linear correlations between the plurality of elements usable to automatically identify and automatically report a denial of service attack without address spoofing.